UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO – EASTERN DIVISION

In the Matter of the Criminal Complaint:
United States of America
V.
KYLE JEFFREY TSCHIEGG
3230 McIntosh Road
Sarasota, Florida 34232

Case No. 2:09-MJ-87
Magistrate Judge Abel

AFFIDAVIT

REDACTED

1. I, Robert E. White II, a Special Agent with the Federal Bureau of Investigation ("FBI"), assigned to the Columbus, Ohio Resident Agency, present the following testament for probable cause of issuance of warrant for the arrest of KYLE JEFFREY TSCHIEGG ("TSCHIEGG"), date of birthxxxx xx, 1970, for interstate transmission of threatening communications and false statements, in violation of 18 U.S.C. §§ 875 (c) (Threatening Communications).

2. Since October 2007 individuals and businesses located in Ohio, Florida, and Kansas have received email, phone calls and text messages whereby the sender threatens to kill or injure the victims and to take over or damage their computers. While as many as 3,500 people may have received copies of the threatening email, the threats themselves were normally directed to a much smaller group; some of the victims included organizations such as "RF Co." (Columbus, Ohio), "Pro" (Sarasota, Florida), "TF" (Brandon, Florida), "Mxx" (Manhattan, Kansas), "Sarasota xxx Church" (Sarasota, Florida), and others. The individuals who received threats included a Florida State Senator "D", "BR" (CEO of "TF"), "EG" (CEO of 'Mxx), "TR" (Assistant Manager at "Pro"), "MT" (Owner of "M Group"), "EC-N" (CEO of "CConsulting") and others.

3. To date more than 180 email messages and 30 telephone calls or text messages have been sent to the victims. Many of the emails were traced back to locations frequented by TSCHIEGG, and video surveillance recorded an individual bearing a strong resemblance to TSCHIEGG purchasing the prepaid cellular phones used to make the threats.

4. Throughout his campaign the subject claimed to have compromised the protected computers and email accounts of the businesses and individuals, and demonstrated knowledge of the contents of those accounts and systems. The subject appears to have a good understanding computer communications and has utilized several techniques hide his identity and location. To further complicate his discovery, the subject has used open wireless access points[1] in several locations to make his initial connections to the Internet.

5. In addition to his fundamental understanding of Internet communications, the subject has demonstrated his familiarity with various email communication methods, Yahoo! Group functionality and management, and webpage construction, hosting and management.

6. According to TSCHIEGG'S public LinkedIn[2] profile, he is an "Independent Computer & Network Security Professional" but has no connections to any professionals in that field. Additional information about TSCHIEGG can be found on the Geocities.com[3] website where TSCHIEGG and his wife "B" share a webpage titled "Tschiegg Creative Design." The site offers links to several web pages that had been created by TSCHIEGG.

Threatening Email which Identified TSCHIEGG

7. The threatening emails were sent to the victims using three methods. Using method one, the subject would either create a new email account or seize control of a victim's email account and use the account to send the threatening email directly to the victims.

8. During his computer security probing of the various Internet-facing victim businesses, the subject likely discovered vulnerabilities in several email servers, which allowed him to reflect email off the servers and have it appear that the email originated from another location or sender. Therefore, using method two, the subject would anonymize any origination information by sending email to the victims through an unsecured, third party email server.

---

[1] Wi-Fi Access Points typically default to an "open" (encryption-free) mode. Novice users benefit from a zero-configuration device that works out of the box, but this default is without any wireless security enabled, providing open wireless access to their LAN. To turn security on requires the user to configure the device, usually via a software graphical user interface (GUI).
[2] LinkedIn is a business-oriented social networking site founded in December 2002 and is mainly used for professional networking. It has more than 30 million registered users, spanning 150 industries.

9. The third method of email communication involved using Yahoo! Groups[4] to terrorize. The subject would create the Yahoo! Group, establish himself as moderator, and then add all of the victims' email addresses to the group. Using this method, the subject could send a single message to the group and it would be received by all of the victims. In addition, as moderator, the subject could control every aspect of the group and the messages posted. If he did not have true control of a victim's email account, the subject would craft or modify an existing group posting so that it appeared to originate from a victim's compromised computer or email account.

10. Since August 2008 "RF Co." has received approximately ten threatening email messages and one threatening phone call. On August 4, 2008, "RF Co." received several threatening emails from kosherguy_1999@yahoo.com:

    a. One message stated "*I want to come to "RF Co." company in columbus and just start shooting the whole place up, blowing your heads off, and then I'm gonna go to "Pro" in sarasota and and kill all of them too, see ya soon!! Im looking forward to painting walls with brain matter :)*"

    b. Another message was titled "howdy!!" and the body of the email stated "*ready to die this afternoon or tonight maybe? I am printing out maps to your places and will soon introduce each of you to my 357 magnum*".

    c. The IP address[5] of the computer used to send the messages was 68.56.199.188, which Comcast Corporation ("Comcast") reported was registered to "DF" of xxxx "Bxxxxx" Drive, Sarasota Florida 3xxxx.

---

[3] Yahoo! GeoCities is a free webhosting service that was founded in 1994.

[4] Yahoo! Groups operate as both electronic mailing lists and Internet forums. Group messages can be posted and read by e-mail or on the Group homepage, like a web forum. Members can choose whether to receive individual e-mails or daily digest e-mails, or to read the posts at the web site. Some Groups are simply announcement lists, to which only the Group moderators can post, while others are discussion lists.

[5] An Internet Protocol (IP) address is a numerical identification (logical address) that is assigned to devices participating in a computer network utilizing the Internet Protocol for communication between its nodes. IP addresses are usually displayed in human-readable notations, such as 208.77.188.166 (for IPv4), and the role of the IP address has been where something is.

11. On August 7, 2008, lpxxxx1552@comcast.net received an email from kosherguy_1999@yahoo.com titled, "Hello "L"" which stated, "*Hey There Sweets! Your friend Ed is dead. He got mixed up with the wrong folks. He was killed by somebody here in pinellas county, they are members of the church of scientology. It was done secretly, everything has been covered up, nobody will ever know or find out what happened or who was involved. I know who killed him, but if i go to the cops i will very likely get killed myself. Anyways, long story short, i got ed's laptop computer. I have been raising some money with the help of it. I know computers very will, i am (not bragging) very good at what i do. My dear, i would like to make a request of you. If you would like to keep your computer working, please consider sending a sum of money to myself at the address indicated below. I would greatly appreciate atleast an amount of $3,000 or more if you want to avoid having your computer hacked into and destroyed by me. I can do it, "L", please be assured that I have the talents and tools to do the job. I have already done it to several people and some local companies. So, bottom line "L", I want atleast three grand ($3,000) in CASH sent to this address as soon as possible. Oh, by the way, DO NOT, DO NOT, DO NOT call the police or anybody else, if i find out you did, i have ways of finding these kind of things out, if i find out the police have been notified about this, i will go ahead and destroy your computer, and i may even consider having a certain person come down to north port to pay you a visit, a visit that will be unforgetable for you and your parents. Leean, please mail CASH of 3g or more to: P.O. Box xxxx Palm Harbor, FL 3xxxx Thank you for your time and attention my sweet lady :) Now send the money. Bye for now."*

12. The IP address of the sending computer was 68.56.199.188, which Comcast reported was assigned to "DF" of xxxx Bxxxxx Drive, Sarasota, Florida 3xxxx. In addition to the examples listed above, at least 44 of the email messages sent by the subject originated from this location.

13. The FBI conducted an assessment of the wireless Internet routers and computers in the vicinity of "DF"s' home at xxxx Bxxxxx Drive, Sarasota, Florida. The assessment showed that inside "DF"s' home there was a wireless access point, which was not secure, that would allow computers in the immediate area to utilize "DF"s' Internet services without their permission.

14. I interviewed "DF", of xxxx Bxxxxx Drive, Sarasota, Florida regarding her home Internet services. She confirmed that she had a wireless Internet router, and that she had not authorized anyone other than her immediate family to access it. With her permission, the FBI installed equipment to record any unauthorized activity in her network.

15. The wireless assessment further showed that a computer located at xxxx Wxxx Avenue (directly behind "DF"s' home) was communicating with their wireless router. xxxx Wxxx Avenue is the address of "MT"'s home and home-based, health coaching business. "MT" is KYLE TSCHIEGG'S father and employer; therefore during the weekdays KYLE TSCHIEGG would routinely be present at xxxx Wxxx Avenue.

16. xxxx Wxxx Avenue is the address of"MT'"s home and home-based health coaching business. "MT" is KYLE TSCHIEGG'S father and employer; consequently during the weekdays KYLE TSCHIEGG would routinely be present at xxxx Wxxx Avenue.

17. During the initial interview, "MT" indicated that he believed the attacker to be "RC", a local businessman. "MT" had rejected "RC's" solicitations to sell him Internet advertising services and shortly thereafter "MT" began receiving threats and experiencing computer problems. "MT" believed "RC" was retaliating against him and KYLE TSCHIEGG enthusiastically supported this theory.

18. According to "MT", no matter what corrective or preventative measures he took, his home computers, email accounts, and phone services were constantly intruded upon or destroyed. "MT" began to rely on KYLE to combat and track the hacker. Eventually "MT" terminated his home Internet service and acquired two laptops that he and KYLE would take to the local library and McDonalds to access the Internet.

19. The United States Postal Service reported that Box xxxx, in Palm Harbor, given in the extortion email above, has been rented by "RC" and his companies, but I believes this information was provided by the attacker to falsely implicate "RC".

20. On September 22, 2008 from 10:47AM to 11:02AM EDT six threatening and harassing emails were sent to victims from a wireless access point at the McDonald's Restaurant at 3901 Cattlemen Road, Sarasota, Florida.

21. Wayport, the Internet Service Provider for the McDonald's, produced records which stated that a computer with the MAC address 00:1A:73:9D:68:D5 had been granted Internet access through the Wayport service on 9/22/2008 from 10:35 AM to 11:53 AM EDT.

22. On December 16, 2008 KYLE TSCHIEGG provided me with system information for the two laptops used by him and his father. In the email, KYLE TSCHIEGG indicated that the HP Pavilion DV9700 laptop named "laptop-PC" was "MT"'s work computer and it had a wireless network card assigned the MAC address 00:21:00:04:B4:63. In another email, KYLE TSCHIEGG indicated that his computer was the HP Pavilion DV6500 laptop named "marvin-PC" and it has a wireless network card assigned the MAC address 00:1A:73:9D:68:D5. The MAC address of KYLE TSCHIEGG'S HP Pavilion DV6500 laptop matched the MAC address of a computer in the McDonald's listed above during the time the threats were emailed.

23. On August 22, 2008, I contacted "Pro" LLC, also called "Pro" xxxxx Group (hereafter referred to as ""Pro""), in Sarasota, Florida and confirmed that it has been receiving similar threatening communications. "Pro" provides wellness and nutrition education to medical professionals, healthcare professionals, nutrition representatives and others. "MT"'s business is one of "Pro"'s customers.

24. Since at least July 3, 2008, "Pro" and some of its employees have received approximately 40 threatening email messages and 30 threatening phone calls or text messages.

25. "TR" (hereafter referred to as ""TR""), the assistant to the "Pro" Co-founder, managed much of the email correspondence and soon became the focus of the threatening messages directed at "Pro".

26. On July 3, 2008, the subject sent an anonymized email to "TR" that stated," *"TR" I am the last person you want to fuck with the things I can do are virtually unlimited, so don't bark up this tree my dear if you mess with me, I will suddenly and seerely become your absolute worst nightmare of all time I have many various capabilities, so if you want to put any of them to the test, please feek welcomed and invited to do so i will come down there to where you are located in Sarasota, when you least expect it, and whatever happens to you will effectively be made to look like an accident also, there is more than one way to skin a cat, my dear there are particular methods that can be used to intrude into your computer, other than*

the ones i have recently tried also, the "TF" company has delusions of invincibilty, as they sit comfortable with the false sense of security they so ignorantly have had i am good enough to penetrate and exploit their system, without them knowing it i have done such things before and they probably never even knew i was in there anyways, bitch, bottom line is dont fuck with me or i will begin executing the consequences upon you with a fervor perviously unrealized i will take down key aspects of your personal and business life still wanna play? if ya do, baby, just keep fuckin with me and we shall soon see what the future holds for you your family your work... you name it bitch and i will fuck you up in so many ways and on so many levels sincerely, potentially your worst fuckin nightmare"

27. When she received the threatening email from the kosherxxxguy_1999@yahoo.com "TR" became very proactive and filed a complaint with Yahoo. She provided them with copies of the threatening communications and Yahoo! terminated the kosherguy_1999@yahoo.com email account, which further enraged the subject. Soon, "TR" began receiving threatening calls on her work, home and cellular phones, as well as occasionally receiving threatening text messages to her cell phone.

28. Google searches revealed a posting to the "rollsroyceownersclub" Yahoo!Group by kosherguy_1999@yahoo.com on November 25, 2002. In the posting, the kosherguy_1999@yahoo.com notified the group that a 1997 BMW 318i was for sale and that additional information can be found at the bmw97.homestead.com webpage. Kosherguy_1999@yahoo.com signed the message "KT." Furthermore, on KYLE TSCHIEGG'S Geocities website described above, under the listing "Designs by Kyle" is a link named "BMW97." The link points to the same webpage (bmw97.homestead.com) given by kosherguy_1999@yahoo.com in the Yahoo! Group posting.

29. On November 19, 2008 Yahoo responded to a search warrant for the kosherguy_1999@yahoo.com account. Because the account had been removed previously no email was available, but Yahoo provided basic account registration information. The account had several alternate identities including kylesarasota@yahoo.com and the alternate email address edboater@comcast.net.

30. When establishing an alternate email address the account owner enters the email address of the alternate identity and a confirmation email is sent to the user. Once the user accepts the

request, the alternate identity is accepted. The edboater@comcast.net account accepted the request on October 24, 2007.

31. On September 25, 2008, "EG", CEO of "Mxx", an Internet business lead company based in Manhattan, Kansas, received an offline message through "Mxxx's website that stated "'*EG', I will wipe out your whole outfit very soon. Think I can't? Watch your back baby! Sleep tight tonight :)*"

32. Later that day, "Mxx" received the following message via the chat service offered to its customers: "*I know where you live. I will blow your head off.*" The IP address was 71.228.87.21, which Comcast reported was assigned to "MM", xxxx N. GulfStream Ave, Apt xxx in Sarasota, Florida.

33. On September 26, 2008 "Mxx" received another threatening chat that stated "'EG' *is going to be killed very soon.*" The IP address was 68.56.4.6, which Comcast reported was assigned to "DF" of xxxx Bxxxxx Drive, Sarasota, Florida 3xxxx.

34. In order to further anonymize himself, the hacker created several Yahoo! Groups accounts: "Pro"inc@yahoogroups.com, "Pro"@yahoogroups.com, "Pro"_2008@yahoogroups.com, "Pro"_com@yahoogroups.com", proevity_941-371-xxxx@yahoogroups.com and "Pro"2008@yahoogroups.com..

35. On October 15, 2008, the subject sent an email through the "TF" email service, which appeared to come from the email account debbieshafferxxxx@yahoo.com. The email was directed to the "Pro"_2008@yahoogroups.com Yahoo! Group account and said, "*If you are reading this email, I have chosen you to be a target. When you least expect it, your head will be invaded with a rifle bullet from a distance, possibly splitting your skull in half or into many fragmented parts. I have a sniper rifle and am fairly decent at hitting my targets. Will I shoot you as you leave for work in the morning? Will I shoot you when you come home from work? Where will I be shooting you from?*" The IP address of the computer that sent the message was 68.56.175.71, which Comcast reported was assigned to a home Internet connection at xxxx Mcxxxxx Road, Sarasota, Florida in the name of "CO"[6].

[6] Sarasota County Property Records show the home in the name of "Cxxxxs O", therefore Comcast records may contain a misspelling.

36. One of the most disturbing emails was sent September 4, 2008, from "TF"u1plus@gmail.com and was written to appear to come from "BR", owner of "TF". In the email the subject attempted to lure "TR" to a remote location, stating "*Hi there "TR", this is "BR". I have just discovered some very important information that I would like to share with you as soon as possible. If it's okay with you, please meet me tonight (Thursday) at 9:00 PM at the open field there by the old Winn Dixie parking lot near the intersection of State Road 70 and North Lockwood Ridge Road in Bradenton, not far from where you live. Please, let's keep this a secret, and don't tell anybody, just show up at that location in person tonight at 9pm. I will meet you there and share this new information privately with you. Thanks and see you there. P.S. I am sending this message to you via somebody else's "TF" video email account, so that we can stay private and hidden from the bad guys.*"

37. On September 25, 2008, "KM" received an email from saul_studmeister@yahoo.com. The email was directed through the Yahoo! Group "Pro"Inc@yahoogroups.com. The subject of the email was "bomb" and the email contained the following text, "*a bomb has been placed near your office building and is set to go off at 2:00 PM EST today...*"

38. On October 6, 2008, the subject sent an email through the "TF" email service that appeared to come from the email account topxx@hotmail.com. The email was directed to the "Pro"Inc@yahoo.com Yahoo! Group account and said, "*Up your fuckin ass.. I got your social security and financial info you homo and other identity You're about to get fucked up the ass....*" Because of the improvements to the "TF" email server the IP address 68.56.4.6 was captured and Comcast reported was assigned to "DF" of xxxx Bxxxxx Drive, Sarasota, Florida 3xxxx in the name of "CO".

39. On October 15, 2008, the subject sent an email through the "TF" email service, which appeared to come from the email account debbieshafferxxxx@yahoo.com. The email was directed to the "Pro"_2008@yahoogroups.com Yahoo! Group account and said, "*If you are reading this email, I have chosen you to be a target. When you least expect it, your head will be invaded with a rifle bullet from a distance, possibly splitting your skull in half or into many fragmented parts. I have a sniper rifle and am fairly decent at hitting my targets. Will I shoot you as you leave for work in the morning? Will I shoot you when you come home from work? Where will I be shooting you from?*" The IP address of the computer that sent the

message was 68.56.175.71, which Comcast reported was assigned to home Internet connection at xxxx Mcxxxxx Road, Sarasota, Florida in the name of "CO".

40. One of the subject's most recent victims has been Florida State Senator "D". The hacker gained control of "D's" email account and in the weeks prior to the November 4, 2008 election and sent numerous messages to the Senator (then State Representative) warning "D" to withdraw from the race:

    a. On October 28, 2008, the subject sent a message to the "Pro"2@yahoogroups.com Group which stated, "*Tell "D" to withdraw from the race or there will be certain materials published that will embarrass and bring shame upon her and her family.*"

    b. On October 30, 2008, the subject sent a message to the thetruthabout"D"@yahoogroups.com Group that stated, "*If you want to keep "D" and "D's" family safe, then you will strongly suggest to "D" that"D" drop out of the race immediately. If 'D" does not drop out, bad things will start to happen to "D" and "D's" family, and also to "D's" campaign people and their families....*"

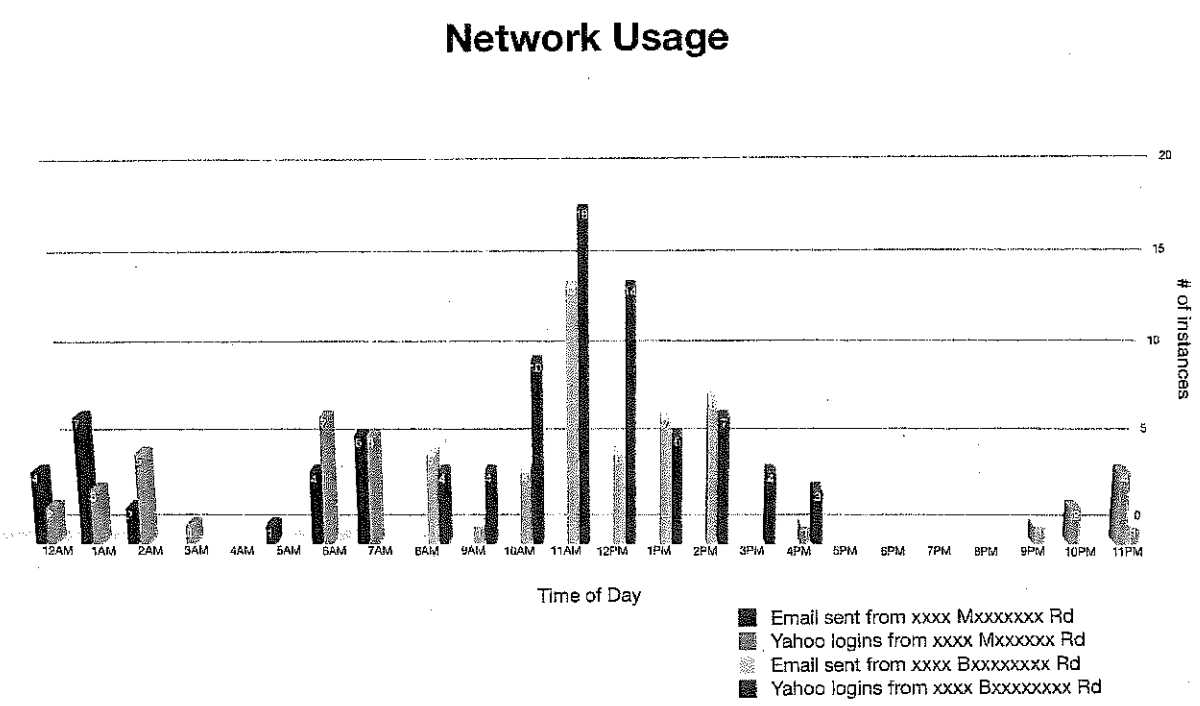
    c. The IP address of the computer that sent the messages was 68.56.175.71, which Comcast reported was assigned to a home Internet connection at xxxx Mcxxxxx Road, Sarasota, Florida in the name of "CO".

41. At least 24 of the emails sent from the subject appeared to originate from the Internet connection located at xxxx Mcxxxxx Road. TSCHIEGG resides at 3230 McIntosh Road, which is 0.01 miles away. The Sarasota County Sheriff's office conducted a wireless assessment of open access points in that area. Like "DF"'s network, "CO's" home network was found to be operating an open wireless access point which would allow other computers in the immediate vicinity to utilize his Internet connection without his knowledge. During the wireless survey, a Sarasota County deputy drove through the immediate neighborhood to determine how far from"CO's" home a computer could be and still access the connection. He found that TSCHIEGG's home was within that range and that TSCHIEGG could have intruded upon"CO's" network and sent the threats from his home.

42. TSCHIEGG'S personal email account is kjt1970@gmail.com and he uses that email to correspond with me under the guise of being one of the victims. GMail provided a login

history for the kjt1970@gmail.com. The history showed that October 28, October 30, and November 7, 2008, TSCHIEGG logged into the kjt1970@gmail.com account using"CO's" network. More importantly, when compared to the IP address login history of the saul_studmeister@yahoo.com account that moderated the victim Yahoo!Groups, it showed that"CO's" network was used to log into TSCHIEGG'S kjt1970@gmail.com account at 5:58AM, then the saul_studmeister@yahoo.com at 6:18 AM, and then again into kjt1970@gmail.com at 7:11AM.

43. An analysis of the available email and the access logs for the kosherguy_1999@yahoo.com and saul_studmeister@yahoo.com accounts showed that throughout the course of this investigation, "DF""s network at xxxx Bxxxxx Road was only accessed from 8:14 AM to 4:57 PM and that Carlos Ochoa's network at xxxx Mcxxxxx Road was only accessed from 10:13 PM to 7:40 AM.



44. The graph above charts the times and locations from which the subject logged into the saul_studmeister@yahoo.com and kosherguy_1999@yahoo.com accounts, and the times and

locations of email threats that was traced back to either "DF""s network (xxxx Bxxxxx Drive) or"CO's" network (xxxx Mcxxxxx Road). As depicted above"CO's" network was accessed late at night and early in the morning and therefore it is reasonable to believe that subject used his laptop from the address listed in this paragraph to access the accounts.

45. On December 8 and 9, 2008 an FBI surveillance team conducted surveillance on xxxx Wxxx Avenue and 3230 McIntosh Road. On December 8, 2008 KYLE TSCHIEGG was observed at 7:55 am departing from 3230 McIntosh Road in a silver GMC Canyon pickup truck. He arrived at xxxx Wxxx Avenue at 8:24 am. At 8:52 am "MT" and KYLE TSCHIEGG were observed traveling from xxxx Wxxx Avenue in the VEHICLE[7] to the Fruitville Public Library. A team member followed the two into the library and observed them at a computer terminal. At 9:21 the two departed the library and returned to xxxx Wxxx Avenue.

46. On December 9, 2008 the surveillance team observed KYLE TSCHIEGG departing 3230 McIntosh Road at 7:56am in a silver GMC Canyon pickup truck. He arrived at xxxx Wxxx Avenue at 8:05am.

47. The VEHICLE is registered in the name of "MT", and has been observed at both xxxx Wxxx Avenue and 3320 McIntosh Road on several occasions, including as recently as February 5, 2009.

48. The observed activity is consistent with work schedule that "MT" described where KYLE TSCHIEGG worked "9 to 5" at xxxx Wxxx Avenue before carrying his laptop computer home with him to 3230 McIntosh Road until his return on the following weekday.

49. On January 1, 2009 "RF Co." reported that the last communication they received from the subject was in October 2008. Their email address appeared to still be a part of the Yahoo! Group account, but the content of the email was not directed toward them.

Threatening Phone Calls, Text Messages and Surveillance Videos which Identified TSCHIEGG

50. Based on interviews with the victims who received threatening phone calls, the caller is described as an adult male, but his voice was distorted by some kind of modulator. At times

[7] One surveillance report incorrectly reported the license number as X629QA and another reported it as X629AQ.

the calls sounded prerecorded while at others appeared to be live. When possible, the victims used Caller ID to identify the calling phone number. They noted the calling numbers were (239) 464-6889, (727) 278-7326, and (239) 565-3376. Additionally, some victims received threatening text messages.

51. On August 7, 2008, the subject purchased a Nokia 1600 cellular phone from the 7-Eleven convenience store #21045 at 5745 Clark Road, Sarasota, Florida. The Nokia 1600 was assigned the phone number (239) 464-6889 and had basic calling and SMS[8] text messaging capabilities.

52. The store surveillance video showed an individual matching TSCHIEGG'S description purchasing the phone with cash. In the surveillance video, the purchaser is wearing a dark and light blue, horizontally striped, collared shirt. Moreover, on TSCHIEGG'S public MySpace[9] webpage he provides a photo album of approximately 40 pictures. The last picture is of KYLE TSCHIEGG wearing the same dark and light blue, horizontally striped, collared shirt.

53. The AT&T detailed call records confirmed that on August 7, 2008, the phone had been used to call 20 people including "TR" and "Pro". The AT&T records supported the victims call records which are given below:

Call sent from (239) 464-6889		
Date	**Recipient**	**Message or Action**
Aug 7, 2008	TR	Hello, I'm going to kill you.
Aug 7, 2008	TR	I'm gonna burn your house down. Burn it down to the ground.
Aug 7, 2008	TR	I'm gonna burn your house down. Im going to burn it down to the ground.

54. According to Ztar Mobile, the cellular service reseller, the phone associated with telephone number (239) 464-6889 experienced a call routing problem, which prevented the phone from receiving calls. Even though more than $10 of service remains on the phone, the owner has

[8] Short Message Service (SMS) is a communications protocol allowing the interchange of short text messages between mobile telephone devices. SMS text messaging is the most widely used data application on the planet, with 2.4 billion active users, or 74% of all mobile phone subscribers sending and receiving text messages on their phones.

not contacted them to resolve the problem and no registration information was available.

55. I believe that this phone became inoperable and was replaced with the Verizon Mobile phone assigned the number (727) 278-7326 on the following day.

56. On August 8, 2008, the subject purchased a Kyocera Marbl cellular phone at the 7-Eleven convenience store #20878 located in Fort Myers, Florida. The purchaser registered the phone to a "RC", P.O. Box xxxx, Palm Harbor Florida 34684. The registration information included the, email address kosherguy_1999@yahoo.com, but no contact phone number was provided. In addition to the basic calling features, the Marbl cellular phone has web browsing and SMS text messaging.

57. The store surveillance video showed an individual matching TSCHIEGG'S description purchasing the phone with cash. I provided the store manager with several pictures of potential subjects and the manager identified KYLE TSCHIEGG as the person who bought the phone. The manager noted that at the time of purchase the customer did not have the mustache exhibited in the photo I provided. In the surveillance video, the purchaser is wearing a dark and light blue, horizontally striped, collared shirt. Moreover, on TSCHIEGG's public MySpace webpage he provides a photo album of approximately 40 pictures. The last picture is of KYLE TSCHIEGG, clean-shaven and wearing the same dark and light blue, horizontally striped, collared shirt.

58. Call records showed that the first call made from the phone was to "B" Tschiegg's unlisted home phone number. Since August 8, 2008, threatening calls have been made from (727) 278-7326. Some of those calls included:

Call sent from (727) 278-7326

Date	Recipient	Message or Action
Aug 8, 2008	TR	I'm going to break into your house this weekend.
Aug 9, 2008	TR	How well do you audit your computer?
Aug 12, 2008	TR	?
Aug 15, 2008	TR	Hey there-
Aug 15, 2008	RF Co.	Going to hack into computers and destroy everything and everyone.
Aug 19, 2008	TR	You dodged a bullet with the storm but you can't dodge me…ha ha ha

[9] MySpace is a social networking website offering an interactive, user-submitted network of friends, personal profiles, blogs, groups, photos, music and videos for teenagers and adults internationally.

59. On November 15, 2008, the subject purchased a Nokia 1600 cellular phone from 7-Eleven convenience store #21045 at 5745 Clark Road, Sarasota, Florida. The Nokia 1600 was assigned the number (239) 565-3376 and has basic calling and SMS text messaging features.

60. The surveillance video of the purchase was obtained from the store security cameras. The video shows a person matching TSCHIEGG'S description purchasing a cellular phone.

61. The AT&T detailed call records confirmed that from November 15, 2008, to November 17, 2008, the phone was used to call at least different 10 people including "TR". The victims provided the following list of threatening calls:

Call sent from (239) 565-3376

Date	Recipient	Message or Action
Nov 15, 2008	BT	He was parked across the street
Nov 16, 2008	EC-N	Send the victim's social security number
Nov 17, 2008	EC-N	I am the hacker in your computer
Nov 17, 2008	TR	You fucking whore.
Nov 18, 2008	TR	I will taunt you with no end in sight and bigger things are being planned for you.
Nov 18, 2008	TR	I am going to kill you very soon
Nov 18, 2008	TR	Your days are numbered
Nov 18, 2008	BT	Called 6-7 times

62. On November 26, 2008 several threatening/harassing text messages were sent to the victims. I analyzed some of the communications on "DF" network for November 25-27, 2008 and found that on November 25, 2008 a computer assigned the MAC address 00:1A:73:9D:68:D5 connected to "DF"'s network and was assigned the IP address 192.168.1.2. The same computer connected to "DF"'s network on November 26, 2008 and was assigned the IP address 192.168.1.3. Again, the MAC address of KYLE TSCHIEGG'S HP Pavilion DV6500 laptop matched the MAC address of a computer used to connect wirelessly to "DF"'s network.

63. During those sessions the subject used that computer to visit various websites including www.txt2day.com (free cellular phone text messaging service), www.telespoof.com (service

which allows you to place a call and spoof[10] your caller ID), www.phonemyphone.com (telephone call reminder service), cellphonemessagesender.com (service to send text messages from a pc to a cell phone), www.phonegangster.com (service to spoof caller ID) and www.stealthrecordercard.com (service to spoof caller ID). Both www.phonegangster.com and www.stealthrecordercard.com offer voice changer and message recording capabilities.

64. On December 30, 2008, "MT" informed me that on the day "MT" went to Dayton, Ohio for a reunion, KYLE reported that the hacker had compromised KYLE'S computer so completely that he was forced to replace the hard drive and to acquire a program capable of hiding or changing his computer's MAC address. When I asked "MT" if he had access to the computer "MT" stated he does not maintain KYLE'S computer and that KYLE takes his laptop home with him each night.

65. It is my belief that KYLE TSCHIEGG replaced the hard drive in his laptop in an effort to conceal his activities and to destroy evidence.

CONCLUSION

66. Based upon the evidence gathered to date, there is probable cause to believe that KYLE TSCHIEGG is responsible for the computer intrusions, extortion and threatening communications directed against victims in Florida, and for threatening communications directed against victims in Ohio and Kansas.

    a. TSCHIEGG'S background is consistent with the computer expertise necessary to conduct the attacks and to conceal his identity.

[10] Caller ID spoofing is the practice of causing the telephone network to display a number on the recipient's caller ID display which is not that of the actual originating station; the term is commonly used to describe situations in which the motivation is considered nefarious by the speaker. Just as e-mail spoofing can make it appear that a message came from any e-mail address the sender chooses, caller ID spoofing can make a call appear to have come from any phone number the caller wishes.

b. TSCHIEGG frequented the locations where the subject accessed the Internet to sent threats, and several network logs confirmed his computer had utilized those resources when threatening messages or malicious activity occurred.

c. Three separate surveillance videos recorded the an individual bearing a strong resemblance to TSCHIEGG purchasing the prepaid cell phones that were used to make telephonic threats, and one store manager identified TSCHIEGG as the purchaser.

_____
Robert E. White II
Special Agent
Federal Bureau of Investigation

SWORN TO BEFORE ME THIS _____ DAY OF FEBRUARY 2009.

_____
Mark R. Abel
United States Magistrate Judge
United States District Court
Southern District of Ohio